Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for authenticating a user's access to a client machine, comprising:

communicating a request for access from the user machine to the client machine;

establishing a login account with login information at the client machine in response to the request;

encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

decrypting the encrypted login information at the authentication server and communicating the decrypted login information to the user machine if the authentication information is acceptable to the authentication server~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

2. (Original) The method of claim 1, further comprising:

communicating an identifier associated with the user from the user machine to the client machine;

encrypting the identifier at the client machine and communicating the encrypted identifier to the user machine;

communicating the encrypted identifier from the user machine to the authentication server; and

decrypting the encrypted identifier at the authentication server;

wherein the decrypted login information is communicated to the user machine if the decrypted identifier is acceptable to the authentication server.

3. (Original) The method of claim 1, further comprising:

encrypting an identifier associated with the client machine at the client machine and communicating the encrypted identifier to the user machine;

communicating the encrypted identifier from the user machine to the authentication server; and

decrypting the encrypted identifier at the authentication server;

wherein the decrypted login information is communicated to the user machine if the decrypted identifier is acceptable to the authentication server.

4. (Original) The method of claim 1, further comprising:

communicating the login information from the user machine to the client machine to enable the user machine to access the client machine.

5. (Original) The method of claim 1, wherein:

the login information comprises at least one of a name and password.

6. (Original) The method of claim 1, wherein:

the login information is encrypted at the client machine using a public key of a public key-private key pair; and

the encrypted login information is decrypted at the authentication server using the private key of the public key-private key pair.

7. (Original) The method of claim 1, wherein:

the authentication information comprises an identifier associated with the user.

8. (Original) The method of claim 1, wherein:

the encrypted login information is inaccessible to the user machine.

9. (Original) The method of claim 1, wherein:

the request for access is communicated from the user machine to the client machine, and the encrypted login information is communicated from the client machine to the user machine via a Secure Sockets Layer connection.

10. (Currently Amended) A system for authenticating a user's access to a client machine, comprising:

means for communicating a request for access from the user machine to the client machine;

means for establishing a login account with login information at the client machine in response to the request;

means for encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

means for communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

means for decrypting the encrypted login information at the authentication server and communicating the decrypted login information to the user machine if the authentication information is acceptable to the authentication server;

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

11. (Currently Amended) A program storage device, tangibly embodying a program of instructions executable by machines to perform a method for authenticating a user's access to a client machine, the method comprising:

communicating a request for access from ~~the~~ a user machine to the client machine;

establishing a login account with login information at the client machine in response to the request;

encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

decrypting the encrypted login information at the authentication server and communicating the decrypted login information to the user machine if the authentication information is acceptable to the authentication server~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

12. (Currently Amended) A method for use at a user machine in authenticating a user's access to a client machine, comprising:

communicating a request for access from the user machine to the client machine;

receiving encrypted login information from the client machine that was generated in response to the request for access;

communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

receiving decrypted login information from the authentication server that was derived by decrypting the encrypted login information when the authentication information is acceptable to the authentication server~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

13. (Original) The method of claim 12, further comprising:

communicating an identifier associated with the user from the user machine to the client machine;

wherein the client machine encrypts the identifier and communicates the encrypted identifier to the user machine; and

communicating the encrypted identifier from the user machine to the authentication server;

wherein the authentication server decrypts the encrypted identifier and communicates the decrypted login information to the user machine if the decrypted identifier is acceptable to the authentication server.

14. (Original) The method of claim 12, wherein the client machine encrypts an associated identifier and communicates the encrypted identifier to the user machine, the method further comprising:

communicating the encrypted identifier from the user machine to the authentication server;

wherein the authentication server decrypts the encrypted identifier and communicates the decrypted login information to the user machine if the decrypted identifier is acceptable to the authentication server.

15. (Original) The method of claim 12, further comprising:

communicating the login information from the user machine to the client machine to enable the user machine to access the client machine.

16. (Original) The method of claim 12, wherein:

the login information comprises at least one of a name and password.

17. (Original) The method of claim 12, wherein:

the login information is encrypted at the client machine using a public key of a public key-private key pair; and

the encrypted login information is decrypted at the authentication server using the private key of the public key-private key pair.

18. (Original) The method of claim 12, wherein:

the authentication information comprises an identifier associated with the user.

19. (Original) The method of claim 12, wherein:

the encrypted login information is inaccessible to the user machine.

20. (Currently Amended) A program storage device, tangibly embodying a program of instructions executable by a user machine to perform a method for authenticating a user's access to a client machine, the method comprising:

communicating a request for access from the user machine to the client machine;

receiving encrypted login information from the client machine that was generated in response to the request for access;

communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

receiving decrypted login information from the authentication server that was derived by decrypting the encrypted login information when the authentication information is acceptable to the authentication server,

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

21. (Currently Amended) A user machine for use in accessing a client machine, comprising:

means for communicating a request for access from the user machine to the client machine;

means for receiving encrypted login information from the client machine that was generated in response to the request for access;

means for communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server; and

means for receiving decrypted login information from the authentication server that was derived by decrypting the encrypted login information when the authentication information is acceptable to the authentication server;

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

22. (Original) The user machine of claim 21, further comprising:

means for communicating an identifier associated with the user from the user machine to the client machine;

wherein the client machine encrypts the identifier and communicates the encrypted identifier to the user machine; and

means for communicating the encrypted identifier from the user machine to the authentication server;

wherein the authentication server decrypts the encrypted identifier and communicates the decrypted login information to the user machine if the decrypted identifier is acceptable to the authentication server.

23. (Original) The user machine of claim 21, wherein the client machine encrypts an associated identifier and communicates the encrypted identifier to the user machine, the user machine further comprising:

means for communicating the encrypted identifier from the user machine to the authentication server;

wherein the authentication server decrypts the encrypted identifier and communicates the decrypted login information to the user machine if the decrypted identifier is acceptable to the authentication server.

24. (Original) The user machine of claim 21, further comprising:

means for communicating the login information from the user machine to the client machine to enable the user machine to access the client machine.

25. (Original) The user machine of claim 21, wherein:

the login information comprises at least one of a name and password.

26. (Original) The user machine of claim 21, wherein:

the login information is encrypted at the client machine using a public key of a public key-private key pair; and

the encrypted login information is decrypted at the authentication server using the private key of the public key-private key pair.

27. (Original) The user machine of claim 21, wherein:

the authentication information comprises an identifier associated with the user.

28. (Currently Amended) A method for use at a client machine for authenticating a user's access to the client machine, comprising:

receiving a request for access from the user machine at the client machine;

establishing a login account with login information at the client machine in response to the request;

encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

wherein the user machine communicates the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine

communicates the encrypted login information and authentication information to the authentication server, and the authentication server decrypts the encrypted login information and communicates the decrypted login information to the user machine if the authentication information is acceptable to the authentication server; and

receiving the login information from the user machine at the client machine to enable the user machine to access the client machine~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

29. (Currently Amended) A program storage device, tangibly embodying a program of instructions executable by a client machine to perform a method for use at the client machine in authenticating a user's access to the client machine, the method comprising:

receiving a request for access from the user machine at the client machine;

establishing a login account with login information at the client machine in response to the request;

encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

wherein the user machine communicates the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server, and the authentication server decrypts the encrypted login information and communicates the decrypted login information to the user machine if the authentication information is acceptable to the authentication server; and

receiving the login information from the user machine at the client machine to enable the user machine to access the client machine~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.

30. (Currently Amended) A client machine in which a user's access to the client machine is authenticated, comprising:

means for receiving a request for access from the user machine at the client machine;

means for establishing a login account with login information at the client machine in response to the request;

means for encrypting the login information at the client machine and communicating the encrypted login information to the user machine;

wherein the user machine communicates the encrypted login information and authentication information associated with the user from the user machine to an authentication server, the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server, and the authentication server decrypts the encrypted login information and communicates the decrypted login information to the user machine if the authentication information is acceptable to the authentication server; and

means for receiving the login information from the user machine at the client machine to enable the user machine to access the client machine~~,~~

no [[link]] direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine.